EXHIBIT S

Contact Us
- Your Local FBI Office
- Overseas Offices
- Submit a Crime Tip
- Report Internet Crime
- More Contacts

Learn About Us
- Quick Facts
- What We Investigate
- Natl. Security Branch
- Information Technology
- Fingerprints & Training
- Laboratory Services
- Reports & Publications
- History
- More About Us

Get Our News
- Press Room
- E-mail Updates
- News Feeds

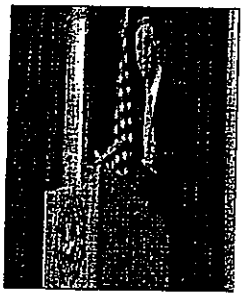
Be Crime Smart
- Wanted by the FBI
- More Protections

Use Our Resources
- For Law Enforcement
- For Communities
- For Researchers
- More Services

Visit Our Kids' Page

Apply for a Job

Major Executive Speeches



John S. Pistole
Deputy Director
Federal Bureau of Investigation

American Bankers Association/American Ba Association Money Laundering Enforcement Conference
Washington, D.C.

October 22, 2007

Note: The Deputy Director may deviate from prepared remarks

Good morning. It's an honor to be here today to talk about terrorist financing and how it affe law enforcement business and the banking business.

Today I want to give you an overview of terrorist financing and walk you through the FBI's pr conducting terrorist financing investigations. And finally, I'd like to talk about how important a are to the FBI's counterterrorism mission.

* * *

Money is the lifeblood of terrorism. Without it, terrorists cannot train, plan, communicate, bu equipment, or execute their attacks. But with it, they can do immeasurable damage. And so always looking for ways to fly below the radar, hoping to stay unnoticed and unsuspected wh turn their plans into a reality.

We learned this lesson the hard way on September 11, 2001. The 9/11 hijackers wanted to unnoticed, and their financial transactions did fly below our radars. It wasn't until after the at when we began backtracking through their finances—that red flags went up.

We discovered that the hijackers used the formal banking system freely and even shared ac accounts. We were able to track their everyday purchases at places like Wal-Mart and their throughout the country. Things that might not have registered before suddenly took on enorm significance. For example, they had no Social Security numbers. They moved their money i relatively small, non-suspicious amounts, using mainly wire transfers and credit and debit ca transactions and some cash transactions.

But they didn't engage in any complex financial tradecraft to conceal their activities. Instead, looked for weaknesses they could exploit. For instance, they sent structured wire transfers f institutions that had no software or program in place to detect them. One financier simply us alias to wire money, because he knew the sending bank didn't have a robust "Know Your Cu program.

Our financial investigation conclusively linked the hijackers together. But it is not enough to financial autopsy after an attack. It became clear that the law enforcement and intelligence

Good morning. It's an honor to be here today to talk about terrorist financing and how it affects the law enforcement business and the banking business.

. Today I want to give you an overview of terrorist financing and walk you through the FBI's process of conducting terrorist financing investigations. And finally, I'd like to talk about how important all of you are to the FBI's counterterrorism mission.

* * *

Money is the lifeblood of terrorism. Without it, terrorists cannot train, plan, communicate, buy equipment, or execute their attacks. But with it, they can do immeasurable damage. And so they are always looking for ways to fly below the radar, hoping to stay unnoticed and unsuspected while they turn their plans into a reality.

We learned this lesson the hard way on September 11, 2001. The 9/11 hijackers wanted to remain unnoticed, and their financial transactions did fly below our radars. It wasn't until after the attacks—when we began backtracking through their finances—that red flags went up.

We discovered that the hijackers used the formal banking system freely and even shared access to accounts. We were able to track their everyday purchases at places like Wal-Mart and their travels throughout the country. Things that might not have registered before suddenly took on enormous significance. For example, they had no Social Security numbers. They moved their money in relatively small, non-suspicious amounts, using mainly wire transfers and credit and debit card transactions and some cash transactions.

But they didn't engage in any complex financial tradecraft to conceal their activities. Instead, they looked for weaknesses they could exploit. For instance, they sent structured wire transfers from institutions that had no software or program in place to detect them. One financier simply used an alias to wire money, because he knew the sending bank didn't have a robust "Know Your Customer" program.

Our financial investigation conclusively linked the hijackers together. But it is not enough to conduct a financial autopsy after an attack. It became clear that the law enforcement and intelligence communities needed to find early opportunities to identify and to disrupt terrorist networks. The best way to do that is to scrutinize finances.

When terrorists raise, store, move, and spend money, they leave trails. They are complex—but they are traceable and identifiable through global financial systems.

The financial analysis of the September 11 hijackers gave us a better idea of what to look for. It helped us establish new intelligence requirements and set up new tripwires. We established a specialized section in our Counterterrorism Division called the Terrorism Financing Operations Section, or TFOS.

The mission of our agents and analysts in TFOS is to trace transactions and track patterns. This painstaking work helps us identify, disrupt, and prosecute terrorists, their associates, their leaders, and their assets.

* * *

Let me give you a sense of how we conduct terrorist financing investigations and what we're looking for. But just a quick reminder that predication is the key to every investigation we undertake. We are not out looking at everyone's finances for no reason. In fact, when it comes to terrorist financing, it is often you who provide the predication for our investigations.

First and foremost, we're looking for basic personal information—addresses, birthdates, phone numbers, and employment. These help us understand day-to-day expenses and spending habits. This information then helps us uncover travel patterns, other accounts, important transactions, and financial histories. And these in turn may lead us to previously unknown business or personal associations, including other members of a network. They may also lead us to discovering criminal activity, such as IRS violations or money laundering.

In short, the most basic financial investigative techniques can result in a gold mine of intelligence.

But we don't want to do a financial autopsy after an attack has occurred. Instead we want to conduct proactive investigations—and we are.

For example, we investigate charities or non-governmental organizations that are used to generate and move money around the world. Some of them fraudulently obtain charitable donations and then divert them to support terrorism.

This was the case with the Benevolence International Foundation in Chicago. It claimed to provide relief to widows and orphans—and it did in fact use some of its funds to provide humanitarian assistance. But the organization was actually a front for al Qaeda. The Executive Director pled guilty to racketeering conspiracy and is now serving 11 years in federal prison.

We also investigate traditional criminal activity that might be used to support terrorism. Because of the crackdown on terrorists and their supporters, terrorists are not necessarily getting stipends from al Qaeda. Instead, they are raising it themselves, often through garden-variety crimes.

For example, the Madrid bombers sold drugs and pirated CDs. A group in North Carolina smuggled cigarettes and used the profits to fund Hezbollah in Lebanon. And in Torrance, California, members of a terrorist cell robbed gas stations so they could buy weapons and plan attacks against Jewish targets and U.S. military installations in Los Angeles. And so we must always be looking for links among traditional crimes and terrorist activities.

Another type of case is one in which we investigate facilitators—the people who move the money, whether witting or unwitting. In addition to using the traditional banking system, terrorists and their supporters also take advantage of unregistered Money Service Businesses and hawalas. These appeal to terrorists and their supporters for obvious reasons. One does not need to be an existing customer to use them.

Hawalas are informal remittance systems that operate primarily within ethnic communities. They can be operated from any location with a phone and Internet hookup, whether it is a gas station or a private home. They don't operate by any of the rules of the financial sector. There is no one to

regulate anything. Hawalas are based on trust and offer near-anonymity for those who are trying to avoid scrutiny. In one case, we investigated a hawala that had sent approximately $4 million to over 20 different customers in foreign countries.

* * *

The 9/11 hijackers proved that terrorists and their supporters are always looking for chinks in the armor of our financial systems. We've made tremendous progress in the past six years in making it much harder for them to raise and move money. A big part of this is thanks to you.
Just like criminals and their money launderers, terrorists and their support networks rely on secrecy to conduct their business. If their activities can be monitored and flagged, they can potentially be stopped. We in the FBI can't do our jobs without the help and cooperation of the banking industry.

You are the gatekeepers of information about terrorists' financial activity. Your compliance with reporting requirements, subpoenas, and other requests for information are absolutely vital to our efforts.

The stronger our systems are, and the closer our coordination is, the better our chances at detecting and stopping terrorists before they can act.

Records produced and maintained pursuant to the Bank Secrecy Act are especially vital weapons in our arsenal—particularly Suspicious Activity Reports and Currency Transaction Reports. Every single one of our terrorism investigations has a financial sub-file—and one of the first things on our checklist is to query FinCEN for BSA reports that match the subject. You would be amazed at how much valuable intelligence they produce—especially SARs and CTRs.

As we have seen since the September 11th attacks, terrorists don't necessarily need huge sums of money to plan and carry out an attack. In a sample of FBI cases, about 42 percent of subjects had BSA reports filed. About 50 percent of those reports reflected transactions of $20,000 or less. This produces a vast amount of financial intelligence.

SARs highlight suspicious behavior and point us to indicators of potential criminal activity—such as structuring and other forms of money laundering. They may be the only hook we have to detect a terrorist cell.

CTRs help fill out the financial intelligence picture because of the objective criteria for filing them. Rather than a subjective analysis of financial behavior, they document specific transactions and patterns of activity that may be the crucial piece of evidence to a case.

CTRs actually provide financial intelligence on more subjects than SARs reporting alone. One tool is not a substitute for the other. SARs and CTRs work in concert together—and together, they are a powerful weapon. Obviously, they provide information about specific transactions. But they provide a much bigger picture than just isolated transactions. They fill in biographical or geographical information—which might let us prove where a suspect was on a particular day. They help us develop leads to expand our investigations. They can link people and accounts conclusively together—connections we might not otherwise see.

Let me give you an example. Some of you may have heard of the Al Haramain Islamic Foundation. It was a charity based in Saudi Arabia, with branches all over the world. Its U.S. branch was established in Oregon in 1997 and in 1999, it registered as a 501(c)(3) charity.

In 2000, the FBI discovered possible connections between Al Haramain and al Qaeda and began an investigation. We started where we often start—by following the money. And we uncovered criminal tax and money laundering violations.

Al Haramain claimed that money was intended to purchase a house of prayer in Missouri—but in reality, the money was sent to Chechnya to support al Qaeda fighters.

In 2004, the Treasury Department announced the designation of the U.S. branch of Al Haramain, as well as two of its leaders, and several other branch offices. In 2005, a federal grand jury indicted Al Haramain and two of its officers on charges of conspiring to defraud the U.S. government.

We relied on BSA information and cooperation with financial institutions for both the predication and fulfillment of the investigation. Because of reporting requirements carried out by banks, we were able to pursue leads and find rock-solid evidence.

Yes, we used other investigative tools—like records checks, surveillance, and interviews of various subjects. But it was the financial evidence that provided justification for the initial designation and then the criminal charges.

That's why your cooperation is so vital—and that of the Treasury Department as well. As in the case I just discussed, together we have frozen the assets of at least 440 suspected and known terrorists or terrorist organizations. We couldn't have done this without the diligence and dedication of the financial institutions that carry out these designations. It is difficult to measure success in convictions of terrorist financiers because of the variety of violations we may use to charge suspects. But it is safe to say that any convictions we achieve absolutely depend on banking information.

So when your bank's officers are conducting reportable transactions, there are some things they can do to help us glean even more information right off the bat. Let me just run through a few:

- You can complete each applicable field.
- You can verify personal identifiers, where possible, and even complete the "description" narrative. When you fill out the "who, what, when, where, why, and how" on the front end, this saves us all time on the back end, because we don't have to come back to you with subpoenas, looking for specific information.
- You can check all the violation types that apply and avoid checking the "other" box.
- Finally, you can file the reports electronically, which will save all of us time.
- And if a customer strikes you as especially suspicious, call us in addition to filing a SAR.

Believe me, we know that this creates a lot of work for you. We also know you don't necessarily

see an obvious return on your investment. But these reports do help us. They often become the cornerstones of our cases. Concrete connections are made by things as innocuous as learning the name of an account's co-signer. The more information we have, the more we have to go on. When we can follow the money, we stand a much better chance of breaking a case wide open.

All of this requires tremendous effort from us all—from your employees and from the FBI's employees. But this cooperation does more than just help us find terrorists and bring them to justice. It helps us all protect the integrity of financial institutions.

* * *

Before I conclude, I want to take a moment to talk about another area of risk, and another way that collaboration can help reduce that risk—and that is in the cyber arena.

We know that terrorists want to wreak havoc on our society, whether by outright attacks on our lives or attacks on our economy. One way in is through cyberspace. Your companies face external risks from terrorists hacking your systems and internal risks from trusted insiders.

We know that hackers have exfiltrated huge amounts of data from the systems of various companies and institutions. The U.S. government is taking strong steps to help shore up vulnerabilities in the .com, .gov, and .edu worlds, and we have identified a number of perpetrators and hardened a number of targets. But as you know, there are always those who are searching for still more vulnerabilities.

Yes, it is your responsibility to protect your systems, but we can help you. Our InfraGard program is a partnership between the FBI and private companies that works to help all of us protect our infrastructure. About two-thirds of Fortune 500 companies are represented, and if you're not a member, we urge you to become one. The InfraGard program lets us share information in a trusted environment on everything from computer intrusions to extortion. If we are all on the same page, we can work with you to investigate the source of the attack and help you guard against another one.

You also face threats from trusted insiders. What if al Qaeda or another foreign sponsor were able to infiltrate someone into your company, perhaps as an IT specialist or systems administrator? The FBI has certainly had a number of applicants for these jobs. Their goal is to get through our screening and get access to our systems. This would be just as dangerous as a truck bomb exploding. These insiders are sophisticated and must be closely watched. Otherwise, they could take down your system, compromise other companies, and cause grave and widespread economic damage.

We all want to protect the privacy of our clients and citizens, yet we also want to protect their security and their lives.

* * *

And so we need to continue our cooperation—and strengthen it. Because more challenges loom ahead, for all of us.

Globalization and technology present new complications. Stored value cards lack regulation and

permit both anonymity and easy transportation of funds. Internet banking also opens up new channels for those wishing to make anonymous transactions. And online payment services don't have even basic customer identification and record-keeping regulations.

And on the opposite end of the technology spectrum, we expect to see cash couriers who can move money without the oversight your institutions provide.

Our adversaries will either become more technologically savvy or they will regress to methods that don't leave a paper trail. We can't predict what they will do. But we can do everything in our power to make it more difficult for them.

Tightening our financial systems works to our advantage and to our enemies' disadvantage. The more we work together, the more we deny them the ability to work in secret and force them to be creative. And the more they are forced to take risks and find ways around our systems, the higher the likelihood they will slip up.

And if they do, we will be waiting to catch them. The threat is real, and the stakes are high. We must not fail. And working together, we will not fail.

###